UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,683	02/08/2002	Nir Zuk	0023-0209	2532

44987 7590 03/28/2007

HARRITY SNYDER, LLP
11350 Random Hills Road
SUITE 600
FAIRFAX, VA 22030

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/072,683	ZUK ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,10,12-18,21-25,27,31-33,35,37-46,49,50 and 52-69* is/are pending in the application.

4a) Of the above claim(s) *8,9,11,19,20,26,28-30,34,36,47,48 and 51* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7, 10, 12-18, 21-25, 27, 31-33, 35, 37-46, 49, 50 and 52-69* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated 1/17/2007 with the amendments to claims 1, 18, 24, 27, 39, 42 and 57 and the cancellation of claims 8-9, 11, 19-20, 26, 28-30, 34, 36, 47-48 and 51.

2. Claims 1-7, 10, 12-18, 21-25, 27, 31-33, 35, 37-46, 49-50 and 52-69 are pending.

Response to Arguments

3. Applicant's arguments filed 1/17/2007 have been fully considered but they are not persuasive. Applicant argues Alexander is not at all related to detecting security breaches and the motivation to combine is improper. Examiner respectfully disagrees, Alexander is directed to data networking and distributing data flows from the high speed source across multiple lower-speed links in a load-sharing manner and mapping of data from the high speed source to the multiple lower-speed links is typically accomplished using a hashing function (see Alexander: 0001-0003). It is proper to combine with other references also dealing with data communication networking.

The applicant argues that Navarro 1997 and Navarro 1998 do not disclose the use of DFA in the manner recited in claims 22 and 39. The examiner respectfully disagrees, claims 22 and 39 recite "querying a signatures database to determine whether there are matching signatures in the TCP stream using deterministic finite automata for pattern matching". Claims 22 and 39 are addressed by the combination of

Gleichauf and Nikander wherein Gleichauf discloses querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (i.e. querying a database to determine whether there are matching signatures in the TCP stream), however it is silent on the capability of using deterministic finite automata for pattern matching. DFA technique is well-known in solving pattern matching problem and it is discussed in "Improving an Algorithm for Approximate Pattern Matching", 1998 (see page 2, 3rd paragraph, 6-7 and 10-15) and "A Partial Deterministic Automaton for Approximate String Matching", 1997 (see Abstract, pages 2-3).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-7, 10, 12-18, 21, 23-25, 27, 31-33, 35, 37-38 and 40-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (6,499,107) and Gleichauf et al. (6,324,656) in view of Nikander et al. (6,253,321) in view of Copeland, III (2003/0105976) and further in view of Alexander et al. (2004/0258073).

a) As to claims 1 and 24, Gleichauf discloses a method and system for adaptive network security using intelligent packet analysis comprising reassembling a plurality of TCP packets in the network traffic into a TCP stream, Gleichauf implicitly

discloses this limitation (i.e. TCP stream reassembly) (col. 6, lines 39-40), to make it even clearer, the examiner takes official notice that use of reassembling TCP packets into a TCP stream is quite well known in data communications network. Data traveling over an IP network is always broken up into packets, the IP protocol adds information to each packet so that the routers along the network know where the data came and where it is going, the packets may be received out of order, or not, and are reassembled in the proper order at the destination computer; inspecting the TCP stream to detect information indicative of a security breach (col. 3, lines 1-4), wherein inspecting the TCP stream to detect information indicative of a security breach (col. 2, lines 50-55) comprises storing a plurality of protocol specifications supported by the network in a protocol database; and querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (col. 6, lines 31-33; col. 8, lines 20-35).

Gleichauf (6,324,656) also discloses inspecting the TCP stream to detect information indicative of a security breach comprises storing a plurality of protocol specifications supported by the network in a protocol database; and querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (Fig. 3B; col. 6, lines 32 – col. 7, line 5).

Gleichauf does not explicitly disclose dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and

forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches.

Nikander is relied on for the teaching of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches (col. 4, lines 41-45).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches in the system of Gleichauf, as Nikander teaches so as to effectively manage communications data.

Gleichauf (6,499,107 and 6,324,656) and Nikander do not specifically disclose grouping the plurality of TCP packets into packet flows and sessions; storing the packet flows in packet flow descriptors and searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream. Copeland is relied on for the teaching of grouping the plurality of TCP packets into packet flows and sessions (paragraphs 0039; 0050); storing the packet flows in packet flow descriptors (paragraph 0050) and searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream (paragraphs 0051, 005, 0081-0083, 0172). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of grouping

the plurality of TCP packets into packet flows and sessions in the system of Gleichauf and Nikander, as Copeland teaches so as to effectively determine if the traffic data appears to be legitimate or possible suspicious activity.

The combination of Gleichauf (6,499,107 and 6,324,656), Nikander and Copeland is silent on the capability of having the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type.

Alexander is relied on for the teaching of discloses packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type (i.e. computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type (page 3, paragraph [0027]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type in the system of Gleichauf (6,499,107 and 6,324,656), Nikander and Copeland as Alexander teaches so as to effectively performing packet filtering.

b) As to claims 2, 12 and 15, Gleichauf discloses inspecting the TCP stream to detect information indicative of security breaches comprising inspecting the TCP stream for protocol irregularities (col. 6, lines 36-42).

c) As to claims 3, 13, and 16-17, Gleichauf discloses inspecting the TCP to detect information indicative of a security breach comprising searching the TCP stream for attack signatures (col. 1, lines 29-31).

d) As to claims 4, 31 and 35, Gleichauf discloses searching the TCP stream for attack signatures comprises using stateful signature detection (col. 6, lines 45-52).

e) As to claims 5, 14 and 33, Gleichauf discloses inspecting the TCP stream to detect information indicative of a security breach using a plurality of network intrusion detection methods (col. 6, lines 66-67).

f) As to claim 6, Gleichauf discloses the plurality of network intrusion detection method comprises at least protocol anomaly detection (col. 6, lines 36-42).

g) As to claim 7, Gleichauf discloses the plurality of network intrusion detection methods comprises at least signature detection (col. 6, lines 43-45).

h) As to claim 10, Copeland discloses searching the packet flow descriptors for traffic signatures and inspecting the TCP stream comprises searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream (page 6, paragraph [0070]).

i) As to claims 18 and 27, Gleichauf discloses a method and system for adaptive network security using intelligent packet analysis comprising reassembling a plurality of TCP packets in the network traffic into a TCP stream, Gleichauf implicitly discloses this limitation (i.e. TCP stream reassembly) (col. 6, lines 39-40), to make it even clearer, the examiner takes official notice that use of reassembling TCP packets into a TCP stream is quite well known in data communications network. Data traveling

over an IP network is always broken up into packets, the IP protocol adds information to each packet so that the routers along the network know where the data came and where it is going, the packets may be received out of order, or not, and are reassembled in the proper order at the destination computer; inspecting the TCP stream to detect information indicative of a security breach (col. 3, lines 1-4).

Gleichauf does not explicitly disclose dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches.

Nikander is relied on for the teaching of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches (col. 4, lines 41-45).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches in the system of Gleichauf, as Nikander teaches so as to effectively manage communications data.

Gleichauf and Nikander do not expressly disclose grouping the plurality of TCP packets into packet flows and sessions, wherein grouping the plurality of TCP packets

into packet flows and sessions comprises storing the packet flows and sessions in a hash table.

Copeland discloses a flow-based intrusion detection system for detecting intrusions in computer communication networks comprising grouping the plurality of TCP packets into packet flows and sessions (Fig. 1, elements "FLOW F1-FLOW F4"; page 5, paragraph [0058]; Fig. 3), wherein grouping the plurality of TCP packets into packet flows and sessions comprises storing the packet flows and sessions in a hash table (page 9, paragraph [0107]), wherein inspecting the TCP stream to detect information indicative of a security breach comprises storing the packet flows in packet flow descriptors (paragraph 0050) and searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream (paragraphs 0051, 005, 0081-0083, 0172).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of grouping the plurality of TCP packets into packet flows and sessions, wherein grouping the plurality of TCP packets into packet flows and sessions comprises storing the packet flows and sessions in a hash table, wherein inspecting the TCP stream to detect information indicative of a security breach comprises storing the packet flows in packet flow descriptors and searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream in the system of Gleichauf and Nikander, as Copeland teaches so as to effectively determine if the traffic data appears to be legitimate or possible suspicious activity.

The combination of Gleichauf, Nikander and Copeland is silent on the capability of having the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type.

Alexander is relied on for the teaching of discloses packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type (i.e. computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type (page 3, paragraph [0027]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type in the system of Gleichauf, Nikander and Copeland as Alexander teaches so as to effectively performing packet filtering.

j) As to claims 21 and 38, Gleichauf discloses searching the TCP stream for attack signatures comprises querying the signatures database to determine whether there are matching signatures in the TCP stream (col. 6, lines 45-52; col. 5, lines 36-42).

l) As to claims 23 and 25, Gleichauf discloses reconstructing the plurality of TCP packets from a plurality of packet fragments (col. 6, lines 39-40).

m) As to claim 32, Copeland discloses a traffic signature detection software module for searching the packet flow descriptors for traffic signatures (page 4, paragraphs [0047-0051]).

n) As to claim 37, Gleichauf (6,324,656) discloses the protocol specifications comprise specifications of one or more of TCP protocol, HTTP protocol, SMTP protocol, FTP protocol, NETBIOS protocol, IMAP protocol, POP3 protocol, TELNET protocol, IRC protocol, RSH protocol, REXEC protocol, and RCMD protocol (Fig. 3B).

o) As to claim 40, Gleichauf discloses a routine for collecting a plurality of security logs and alarms recording information about security breaches found in the TCP stream (col. 7, lines 1-5); a routine for storing a network security policy identifying the network traffic to inspect and a plurality of network attacks to be detected and prevented (col. 5, lines 33-42); a routine for distributing the network security policy to one or more gateway points in the network (Fig. 2, element 20) and a routine for updating the protocol database and the signatures database (col. 9, lines 7-13).

p) As to claim 41, Copeland discloses the system further comprising a graphical user interface comprising a routine for displaying network security information to network security administrators; and a routine for specifying a network security policy (page 11, paragraph [0182]).

6. Claims 22 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (6,499,107) and Gleichauf et al. (6,324,656) in view of Nikander et al. (6,253,321).

Gleichauf discloses a method and system for adaptive network security using intelligent packet analysis comprising reassembling a plurality of TCP packets in the network traffic into a TCP stream, Gleichauf implicitly discloses this limitation (i.e. TCP stream reassembly) (col. 6, lines 39-40), to make it even clearer, the examiner takes official notice that use of reassembling TCP packets into a TCP stream is quite well known in data communications network. Data traveling over an IP network is always broken up into packets, the IP protocol adds information to each packet so that the routers along the network know where the data came and where it is going, the packets may be received out of order, or not, and are reassembled in the proper order at the destination computer; inspecting the TCP stream to detect information indicative of a security breach (col. 3, lines 1-4), querying a signatures database to determine whether there are matching signatures in the TCP stream (col. 6, lines 45-52; col. 5, lines 36-42).

Gleichauf does not explicitly disclose dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches.

Nikander is relied on for the teaching of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches (col. 4, lines 41-45).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches in the system of Gleichauf, as Nikander teaches so as to effectively manage communications data.

Gleichauf and Nikander do not expressly disclose using deterministic finite automata for pattern matching when querying a signatures database to determine whether there are matching signatures in the TCP stream.

The examiner takes official notice that use of deterministic finite automaton for providing a pattern matching is well known in the theory of computation.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of deterministic finite automaton for providing a pattern matching is well known in the theory of computation in the system of Gleichauf and Nikander so as to effectively implementing pattern matching.

7. Claims 42-46, 49-50 and 52-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (6,499,107) in view of Nikander et al. (6,253,321) in view of Trcka et al. (6,453,345) in view of Copeland, III (2003/0105976) and further in view of Alexander et al. (2004/0258073).

a) As to claims 42 and 57, Gleichauf discloses a method and system for adaptive network security using intelligent packet analysis comprising reassembling a plurality of TCP packets in the network traffic into a TCP stream, Gleichauf implicitly

discloses this limitation (i.e. TCP stream reassembly) on col. 6, lines 39-40, to make it even clearer, the examiner takes official notice that use of reassembling TCP packets into a TCP stream is quite well known in data communications network. Data traveling over an IP network is always broken up into packets, the IP protocol adds information to each packet so that the routers along the network know where the data came and where it is going, the packets may be received out of order, or not, and are reassembled in the proper order at the destination computer; inspecting the TCP stream to detect information indicative of security breaches (col. 3, lines 1-4), wherein inspecting the TCP stream to detect information indicative of a security breach (col. 2, lines 50-55) comprises storing a plurality of protocol specifications supported by the network in a protocol database; and querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (col. 6, lines 31-33; col. 8, lines 20-35).

Gleichauf (6,324,656) also discloses inspecting the TCP stream to detect information indicative of a security breach comprises storing a plurality of protocol specifications supported by the network in a protocol database; and querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (Fig. 3B; col. 6, lines 32 – col. 7, line 5).

Gleichauf does not disclose dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach and forwarding a TCP

packet to a network destination if the TCP stream does not contain information indicative of a security breach.

Nikander discloses dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of a security breach (col. 4, lines 41-45).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of a security breach in the system of Gleichauf, as Nikander teaches so as to effectively manage communications data.

Gleichauf and Nikander do not disclose a central management server and a graphical user interface.

Trcka discloses a network security and surveillance system comprising a central management center (col. 15, lines 13-21; Fig. 8, element 64) to control the network intrusion detection and prevention sensor and a graphical user interface for configuring the network intrusion detection and prevention sensor (col. 13, lines 50-65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ to use of having a central management server to control the network intrusion detection and prevention sensor and a graphical user interface for configuring the network intrusion detection and prevention sensor (col. 13, lines 50-65)

in the system of Gleichauf and Nikander as Trcka teaches so as to detect and protect against security breaches, network failures and other types of data compromising events (col. 1, lines 10-15).

Gleichauf, Nikander and Trcka do not specifically disclose grouping the plurality of TCP packets into packet flows and sessions; storing the packet flows in packet flow descriptors and searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream. Copeland is relied on for the teaching of grouping the plurality of TCP packets into packet flows and sessions (paragraphs 0039; 0050); storing the packet flows in packet flow descriptors (paragraph 0050) and searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream (paragraphs 0051, 005, 0081-0083, 0172). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of grouping the plurality of TCP packets into packet flows and sessions, wherein grouping the plurality of TCP packets into packet flows and sessions comprises storing the packet flows and sessions in a hash table in the system of Gleichauf, Nikander and Trcka, as Copeland teaches so as to effectively determine if the traffic data appears to be legitimate or possible suspicious activity.

The combination of Gleichauf, Nikander, Trcka and Copeland is silent on the capability of having the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type.

Alexander is relied on for the teaching of discloses packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type (i.e. computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type (page 3, paragraph [0027]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type in the system of Gleichauf, Nikander, Trcka and Copeland as Alexander teaches so as to effectively performing packet filtering.

b) As to claims 46 and 59, Nikander discloses dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of a security breach (col. 4, lines 41-45).

c) As to claims 50, 54, 66 and 69, Gleichauf discloses searching the TCP stream for attack signatures comprises using stateful signature detection (col. 6, lines 45-52).

d) As to claims 52 and 67, Gleichauf discloses inspecting the TCP stream to detect information indicative of a security breach using a plurality of network intrusion detection methods (col. 6, lines 66-67).

e) As to claim 49, 53, 65 and 68, Gleichauf discloses the plurality of network intrusion detection method comprises at least protocol anomaly detection (col. 6, lines 36-42).

f) As to claims 45 and 58, Gleichauf discloses reconstructing the plurality of TCP packets from a plurality of packet fragments (col. 6, lines 39-40).

g) As to claims 55, 60 and 63-64, Gleichauf discloses a routine for collecting a plurality of security logs and alarms recording information about security breaches found in the TCP stream (col. 7, lines 1-5); a routine for storing a network security policy identifying the network traffic to inspect and a plurality of network attacks to be detected and prevented (col. 5, lines 33-42); a routine for distributing the network security policy to one or more gateway points in the network (Fig. 2, element 20) and a routine for updating the protocol database and the signatures database (col. 9, lines 7-13).

h) As to claims 56, and 61-62, Copeland discloses the system further comprising a graphical user interface comprising a routine for displaying network security information to network security administrators; and a routine for specifying a network security policy (page 11, paragraph [0182]).

i) As to claim 43, Gleichauf discloses the network intrusion detection and prevention sensor is placed inside a firewall (col. 4, lines 47-49).

j) As to claim 44, Gleichauf discloses the network intrusion detection and prevention sensor is placed outside a firewall (col. 5, lines 24-27).

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
3/21/07

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER